PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10 | A1

(11) International Publication Number: WO 99/19845

(43) International Publication Date: 22 April 1999 (22.04.99)

(21) International Application Number: PCT/US98/19717

(22) International Filing Date: 21 September 1998 (21.09.98)

(30) Priority Data:
60/060,643 1 October 1997 (01.10.97) US

(71) Applicant: AT & T CORP. [US/US]; 32 Avenue of the Americas, New York, NY 10013–2412 (US).

(72) Inventor: MAHER, David, P.; 117 Old Mill Court, Ponte Vedra Beach, FL 32082 (US).

(74) Agents: DWORETSKY, Samuel, H. et al.; AT & T Corp., P.O. Box 4110, Middletown, NJ 07748 (US).

(81) Designated States: BR, CA, MX, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A METHOD AND APPARATUS USING DIGITAL CREDENTIALS AND OTHER ELECTRONIC CERTIFICATES FOR ELECTRONIC TRANSACTIONS

(57) Abstract

A method for performing electronic transactions, comprising receiving a long–term certificate, authenticating a user associated with the long–term certificate, and then sending a short–term certificate to the authenticated user. In addition, risk associated with the user can be evaluated, and this risk information, as well as other information, can be included in the short–term certificate.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

A METHOD AND APPARATUS USING DIGITAL CREDENTIALS AND OTHER ELECTRONIC CERTIFICATES FOR ELECTRONIC TRANSACTIONS

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims priority to Provisional Application Serial No. 60/060643, filed on October 1, 1997.

FIELD OF THE INVENTION

The present invention relates to digital credentials and other electronic certificates. More particularly, the present invention relates to a service for using digital credentials and other electronic certificates to practice commerce on a network.

BACKGROUND OF THE INVENTION

To exercise certain rights and privileges, people need to possess or show various types of credentials. Credentials are certificates such as birth certificates, Social Security Cards, driver's licenses, membership cards, admission badges, charge cards, and the like that represent some certified assertion about a person. In the case of a driver's license, an officer of the state certifies that a specific person is licensed to drive a vehicle. A charge card represents an assertion, certified by some bank or other organization, that a person has a charge account at that bank. Companies issue credentials for their employees, usually in the form of ID badges. Generally, the certificate will include some means of identifying to whom the assertion applies (the holder or subject of the credential), and who is certifying the assertion (the certifier of the credential, who is often the issuer).

In the case of a driver's license or corporate ID, the holder is typically identified by a photograph and signature specimen laminated

to the certificate and the certifier of the credential is usually identified by a logo, layout, and some other means such as a hologram.

With the advent of electronic commerce, standard credentials have become insufficient, and the need for digital credentials has become more widespread. Digital credentials are electronic certificates having the property that the assertions about the holder can be interpreted and verified by a computer, the certifier can be reliably recognized by a computer, and the holder's present intention to use the credentials can be recognized by a computer (often remotely, through a network). Digital credentials can use a cryptographic mechanism known as a digital signature. An electronic document can be signed by applying a cryptographic secret key controlled by the signer. A signature can be verified using public information (known as the public key). The verification process can use the public key to verify that the signer's secret key was used to sign the document. The science of public key cryptography enables this.

Examples of digital credentials are automatic teller machine (ATM) or bank cards. As opposed to other types of certificates mentioned earlier, these are not usually presented to people for verification. They are normally presented to an ATM and ultimately to a specialized computer network. The relevant information regarding the certifier is digitally encoded on a magnetic strip and the cardholder is identified by a Personal Identity Number or PIN. Furthermore, the holder's present intention to apply the rights asserted by the credential (such as withdrawing money) is signified by the holder's entry of the PIN. This ATM card allows the holder to use electronic banking over specialized digital networks. The present form of digital credentials, however, can support only a minimal variety of services over specialized and non-specialized networks such as the Internet.

Present ways of using digital credentials (using PINs and

passwords) are notoriously insecure, very user-unfriendly, and generally inadequate for electronic commerce. For example, while hand-written signatures on documents can make paper records auditable, PINs and passwords are not very useful for this purpose. In particular, they do not have persistent properties as signatures do. For example, one can directly verify a signature post-hoc, but PINs and passwords can be verified only at time of use. The certified digital signature can substitute for a hand-written signature.

The importance of digital credentials is rapidly increasing because networks are becoming more open and public. Whereas a person's identity on a closed network is known through a network operating system, and privileges can be determined by database look-ups, such is not the case on the Internet, for example.

Digitally-signed certificates have been used in electronic payment systems that have arisen over the past five years or so. At least three distinct types of payment systems exist, each of which differs from the current invention in significant ways. The three systems are referred to as e-check, e-charge, and e-cash.

An e-check is designed to function in a way similar to the way paper checks function. While a paper check is a signed request for a bank to pay a given amount from the payer's account to the party that is named on the check (the payee), an e-check is a message requesting the same procedure, but it is electronically signed by the payer. The electronic signature certifies, as in the case of a paper check that the user attests to the payment request and to the specifics of the payee and the amount. With a paper check, the payee has the option of verifying the identity of the payer in person, often demanding one or more alternate methods of payer identification, or the payee can sometimes wait until the check "clears" before providing value in return for the check. Clearing means that the payee's bank receives payment from the payer's

bank. With an e-check system, the payee can also wait until the check clears from the payer's bank, or the payee can accept the legitimacy of the payer's digital signature by checking the certificate that the payer's bank issues to the payer which certifies the payer's signing key. In the latter case, the payee risks the possibility that the digital signature certificate has been revoked. This risk is reduced when the payee checks an electronic "Certificate Revocation List" or CRL. Nonetheless, the residual risk exists that the CRL is not up to date. Additionally, the traditional risk exists that the payer's account may have insufficient funds, and the e-check will not clear.

E-checks use the same clearing system and clearing networks used by paper checks. The systems and networks are relatively expensive to use, and when one adds the cost of administering CRLs and the cost of processing e-checks returned for insufficient funds, the use of e-checks for relatively small payments of a few dollars or less is not cost effective. In the present invention, these inefficiencies are addressed by reducing the dependency on CRLs, and by use of a novel approach to risk management, integrating risk management parameters directly into a certificate.

Another use of digital certificates in payment systems is illustrated by the Secure Electronic Transaction ("SET") standard that has been proposed by MasterCard and Visa. SET describes a relatively complex mechanism for making a payment using certificates within the current credit card payment support infrastructure. A number of parties exist in SET: the cardholder, the payee (or merchant), the issuing bank, the acquirer (or merchant's bank), the payment gateway, and optionally, "third parties" that represent one or more of the financial institutions involved. In SET, five different parties have certificates. Cardholder certificates function as an electronic representation of the payment card. Merchant certificates function as an electronic substitute for the

payment brand decal that appears in a store window. Payment Gateway certificates are used by Acquirer's or their processors for the systems that process authorization and capture messages. In addition, Acquirer certificates and Issuer certificates aid in the distribution of Merchant and Issuer certificates, respectively. In general, the various certificates are used to support cryptographic keys that are used to provide credit card transaction messages with security properties such as privacy and authenticity.

SET is, overall, an elaborate scheme that is described in the "SET Secure Electronic Payment Transaction Specification" published by MasterCard and Visa. The certificates involved in SET may need to be revoked for any of a number of reasons such as key compromise, or change of status of the party holding the certificate. In contrast to the present invention, the scheme requires a certificate hierarchy, on-line verification procedures, and a certificate revocation infrastructure. Transactions require a significant amount of computation by multiple parties to complete.

Another use of digital certificates in payment systems is illustrated in electronic cash (e-cash) systems where cash is either represented by digital bearer certificates or by "value registers" in smart cards. In the case of digital bearer certificates, a digital signature is applied to an assertion that the certificate may be redeemed for a certain amount of cash at a certain bank or financial institution. A bank will issue certificates that can be used to verify the authenticity of the signature on the bearer certificate. Because digital bearer certificates can be freely copied, a risk exists that users will attempt to repeatedly use the same certificate. Therefore, risk management measures must be employed to ensure that each certificate is spent precisely once. Typically, either a smart card is used to contain the certificates and to participate in a two party protocol that marks certificates as used, or a

network-based mechanism may be employed that records each certificate as it is used, and allows any payee to see if the certificate tendered is being used for the first time.

In the case of value registers in smart cards, certificates are used to certify the keys used to verify the digital signatures on messages that are exchanged between two software applications running on the smart cards. For example, a payer's smart card debits its value register (or current cash balance), and signs and sends a message affirming the act to the payee. The payee, upon receiving the message affirming the debit can check the signature on the certificate and verify the signature on the message.

Multiple risks exist in this system as well. In particular, the credit and debit operations must be encapsulated within smart cards or some other physically secure containers that must be distributed and maintained. In addition, should the certificates be compromised, counterfeit e-cash can be produced that is indistinguishable from e-cash that is issued by a legitimate originator. Should the physical container of a card be compromised, then clones of that card could be created that never debit their balances but nonetheless dispense e-cash acceptable to other cards. These are called "golden goose" cards. Thus, this type of e-cash, as a payment system, requires significant risk management measures. Another difficulty associated with this payment scheme has to do with recovery from errors. A communication error can literally destroy value. For example, if one smart card sends a signed message "I have debited my value register by $20" to another smart card, yet the second smart card does not receive that message intact, no credit will be offset to the debit. A support structure to make amends for these type of errors is required.

The shortcomings with the prior art involve the difficulty in using credentials that have been distributed electronically in a highly

distributed system that lacks a reasonable means to revoke or update the credentials. For example, assume one holds a digital credential that authorizes the holder to purchase goods up to a value of one hundred thousand dollars (e.g., a corporate credit card). To use this credential, one must go to a central database to re-verify each time the credential is used.

Within the known systems, risk management measures are required to properly support payment systems, and defend them against fraud. Yet the known systems do not contain an efficient way in which risk management is integrated into the payment system.

SUMMARY OF THE INVENTION

The present invention relates to a method and apparatus for using digital credentials, or certificates to facilitate commerce on a network. In one embodiment of this invention, a party wishing to act as guarantor of a transaction would receive long-term certificates from a consumer after the consumer logs into the network. The guarantor analyzes the long-term certificates, at least to verify the identity of the consumer. The guarantor, after being satisfied with the information presented, supplies short-term certificates containing assertions based on information from the above analyses. The short-term certificates can then be used to purchase goods from participating merchants on a network.

In another embodiment, merchants use the short-term certificates to verify terms and conditions under which a given consumer can be billed through the guarantor. The short-term certificates also certify the cryptographic public keys of consumers that are used to digitally sign statements requesting merchants to bill for goods and services purchased through the guarantor. Billing records associated with purchases are forwarded to the guarantor or his agent, whereby the records are sorted

by consumer identity and used to construct periodic statements containing many billing records that are made available to consumers who can make a single payment. Detailed information about the purchases is thus provided to the guarantor who then helps merchants market goods accordingly. The billing records may contain digitally signed statements by consumers directing the merchant to bill through the guarantor.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 illustrates a system-level block diagram of an embodiment of the present invention.

FIGURE 2 is a flow chart of an embodiment of a method of the present invention.

FIGURE 3 illustrates an embodiment of an apparatus and system in accordance with the present invention.

DETAILED DESCRIPTION

The present invention is directed to ways of using digital credentials and other electronic certificates to practice commerce over a network. The purpose is to run a relatively convenient and efficient system using a combination of both long-term and short-term certificates.

Long-term certificates, as defined here, are certificates that contain information or make an assertion that is not expected to change over some long period of time. For example, long-term certificates can be used to represent a person's identity. Revocation of long-term certificates is not necessary on any large scale because the information contained in long-term certificates is relatively static and benign.

Short-term certificates, on the other hand, hold information or make assertions that may rapidly change, and therefore are designed to

expire after some relatively short period of time. For example, short-term certificates may contain information about a person's credit history, shopping history, or information about the short-term certificate's maximum value as currency. Short-term certificates may make assertions about what a person is authorized to do, or about agreements that they may have with other parties.

The validity of the short-term credentials can be based on an individual's identity. For example, when a person logs into a system, the person uses some means to verify identity (using long-term credentials, for example), and then the system supplies short-term credentials which say, for example, that the client is authorized to charge for commerce on the world wide web for purchases the amount of which is not to exceed some fixed amount. Typically the short-term credential can also certify cryptographic keys that can be used for digital signatures that affirm a person's agreement with a contract. In addition, the short-term credential might contain the semantics attributed to the use of the person's digital signature as well as statements of limitations of liability.

Referring now in detail to the drawings, Figure 1 illustrates a system-level embodiment of the present invention. In this system, Customer Client 104 desires to purchase goods or services from Merchant 105. To do this, Customer Client 104 needs to present to Merchant 105 a form of payment that will be accepted by Merchant 105. In anticipation of this, Client 104 may present a long-term certificate to a certifier to access a certificate of payment called a short-term certificate.

The long-term certificate can be certified through known encryption techniques. The certifier is typically, for example, an internet service provider, bank, or any entity designed to certify credentials. The long-term certificate contains, at the very least,

information that verifies the identity of Customer Client 104. The long-term certificate may contain other information desired by the certifier. Once the certifier is satisfied by Customer Client 104's long-term certificate information, the certifier sends Customer Client 104 one or more short-term certificates from the short-term certificate database 103.

Short-term certificates are digital in form, and contain information stating, at least, that the certifier guaranties payment up to a certain amount of value. In addition, the short-term certificate can contain marketing information. For example, a short-term certificate can tell a participating merchant that goods and services may be charged by the client named in the certificate to a specific account, through an agreed-upon channel, for up to the amount of $20. In addition, the short-term certificate may contain information that instructs Merchant 105 to apply a 20% discount to the cost of the goods supplied to the bearer of this short-term certificate. Upon receiving a short-term certificate, Merchant 105 can send an optional query to the short-term database for various reasons such as double-checking the certificate's validity in the case when the purchase amount exceeds some threshold stated in the short-term certificate. The short-term certificates are short term in the sense that they contain information or make assertions based on information that may change over a relatively short period of time. They therefore can be set to expire in some short period of time. For example, a certifier may supply a short-term certificate to Customer Client 104 that guaranties that the Client can charge to an account the purchase of any item that costs up to $20, but can only be used within 24 hours after Customer Client 104 receives this certificate.

Merchant 105 and Customer Client 104 consummate a transaction by promising (on the part of Merchant 105) to supply goods or services in exchange for an affirmative indication on the part of the Client that the goods or services can be charged to a billing account

maintained in Billing System 106 according to and limited by the information provided by a short-term certificate. Once the short-term certificate is received, and the transaction is completed, the short-term certificate is sent along with an electronic record of a bill of sale through agreed-upon channels for payment from the certifier, or guarantor.

The above-mentioned agreed-upon channels, called Billing System 106, collect billing records, and their corresponding short-term certificates and renders them for payment. In addition to serving as a conduit for payment, the billing system may supply information to various subsystems that serve to analyze information about the transaction. The Transaction Analysis 107 collects details of the transaction. The Transaction Analysis 107 correlates different types of purchases with different demographics of this particular Customer Client 104, and then determines what offers might be made to this particular consumer. The purpose of the transaction analysis is to determine patterns of consumer behavior so that some action may be taken. For example, Customer Client 104 might show a pattern of behavior that would alert the certifier that Customer Client 104 is in the market for an automobile. In other words, transactional information is used to better match marketing with consumer-behavior information.

Once the transactional analysis is complete, the results are used in Offer Management 102 to market goods or services to Customer Client 104, possibly by attaching offers to short-term certificates in Short-Term-Certificate Database 103. In this way, a type of high-gain feedback loop is completed, as can be seen in FIGURE 1. In FIGURE 1, Offer Management 102 can use information received by Risk Management System 102(a), Loyalty System 102(b), and Market Partners 102(c) to determine what, if any, information should go into the short-term certificates along with any assertions that might be made

about terms and conditions, credit limits, discounts, etc. Risk Management System 102(a) can receive information from Billing System 106, thereby keeping data on a particular Customer Client's usage patterns. Risk Management System 106 can then analyze the information supplied by Billing System 106, and alert the certifier as to how much risk should be taken with regard to a particular Customer Client. For example, Risk Management System 102(a) can alert the certifier to change the credit limit, either up or down, for a particular Customer Client. The system also can determine whether or not the recent usage patterns of a person are indicative of fraud or other misuse (that may have resulted from a key management compromise whereby a consumer's identity certificate and secret key have been compromised). This information passed between Billing System 106, Risk Management System 102(a), and the certifier can be updated and analyzed arbitrarily quickly, possibly on a daily basis. This rapid response obviates the need for use of certificate revocation lists.

Billing System 106 can also supply information to Loyalty System 102(b). Loyalty System 102(b) is a system whereby consumers are rewarded for regular use of a particular merchant. An example of a loyalty system is found in frequent-flier programs. Loyalty System 102(b) can collect and analyze information, and then supply this information to the certifier's Offer Management 102 so the certifier can tailor its marketing through Offer Management 102 accordingly. In particular, the Offer Management process can author assertions to be inserted into the short-term certificates that declare that loyalty points are available to pay for purchases from participating merchants. Such a merchant can thus accept payment ostensibly in loyalty points, but the merchant can be remunerated through the billing system in cash or other consideration upon presentment of a certificate-backed, signed purchase agreement. This system offers an advantage over other loyalty systems

because one purpose of a loyalty system is to reinforce good behavior by rewarding the user, and this system can reward the user arbitrarily rapidly.

Market Partners 102(c) can enter into agreements with certifiers to help the certifier tailor its marketing through Offer Management 102. The idea is to capture the value of transactional information without severely impacting the consumer's privacy. Market Partner 102(c) provide information to the system about what Market Partner 102(c) desires in a consumer. This information might be a demographic profile, a consumer-behavior profile, etc. For example, Market Partner 102(c) can tell the certifier that it wishes to target people who are shopping for new cars. Offer Management 102 then correlates the needs of Market Partner 102(c) with the information it contains about the consumer.

Figure 2 is a flow chart of a process in accordance with an embodiment of the present invention. In its most basic form, long-term certificates, or some other proof of identity are received by the certifier at step 200. At step 201, the certifier then analyzes the information presented in the long-term certificate and then, at step 202, supplies, from a short-term-certificate database, short-term certificates that can be used as instruments to purchase goods from merchants on the network.

In addition to receiving long-term certificates, the certifier may receive, at step 203 information from a billing system, at step 204 information from a market partner, and at step 205 information from a loyalty system.

The short-term certificate can contain a maximum value for which certifier will act as guarantor upon presentment by a merchant. In addition, the short-term certificate can contain information about offers to the consumer, incentive programs, or loyalty programs.

As stated above, various subsystems, such as a risk management system, a loyalty system, or a marketing system can be interposed between the certifier and the merchant. The short-term certificate can contain information reflecting, for example, the risk-management analysis with regard to a consumer, the loyalty-system analysis with regard to a consumer, or the marketing analysis with regard to the consumer. For example, the short-term certificate can contain a limit on the certificate's guaranty limits based on the risk-management analysis; the certificate can contain a number of acquired consumer points based on the loyalty-system analysis; and the certificate can contain offers (including incentives) to the consumer based on the marketing analysis.

When a consumer desires to make a purchase from a participating merchant, he or she presents through the network one or more short-term certificates. The merchant can analyze the short-term certificate, and determine any guarantees of payment, any rights to use alternative methods of payment such as loyalty points, any discounts or other entitlements, and then make appropriate adjustments to the consumer's bill of sale. The merchant's final price, terms, and conditions for a sale as part of a bill-of-sale, are forwarded to the consumer, who will indicate acceptance, and make the purchase through some affirmative act (that may be required by a condition stated in the short-term certificate) such as signing the bill of sale with a digital signature whose verification key is certified by the short-term certificate.

Ultimately, the certifier can collect for the goods or services furnished guaranteed by creating a billing record containing references to sending the bill of sale and the short-term certificate obtained from the user, and forwarding this billing record through a regular billing channel to the certifier. The certifier can then collect all billing records associated with a specific user and present them to the user in a statement. For example, if the certifier is a telephone company, the

telephone company can bill the user for amounts as stated in the short-term certificate by using the user's regular monthly telephone bill.

FIGURE 3 shows an embodiment of an apparatus in accordance with the present invention. The apparatus includes processor 301, memory 302 that stores instructions adapted to be executed by processor 301, and port 303 adapted to be connected to a network, with both port 303 and memory 302 coupled to processor 301. Memory includes any medium capable of storing instructions adapted to be executed by a processor. Some examples of such media include, but are not limited to, floppy disks, CDROM, magnetic tape, semiconductor memory, hard drives, and any other device that can store digital information. In one embodiment, the instructions are stored on the medium in a compressed and/or encrypted format. As used herein, the phrase "adapted to be executed by a processor" is meant to encompass instructions stored in a compressed and/or encrypted format, as well as instructions that have to be compiled or installed by an installer before being executed by the processor.

In one embodiment of the present invention, memory 302 stores instructions adapted to be run on processor 301, to receive information, analyze that information, and then supply short-term certificates the character of which depends on the results of the analysis. The information received and analyzed can come from market partners, a billing system, a loyalty system, and from long-term certificates supplied by a consumer.

As explained in detail above the invention increases efficiency and productivity of commerce on a network. By using digital credentials and other digital certificates, micro-billing becomes more feasible by decreasing transaction costs, limiting risk, and allowing for easily updated credentials.

Although various embodiments are specifically illustrated and

described herein, it will be appreciated that modifications and variations of the present invention are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention.

5

WHAT IS CLAIMED IS:

1. A method for performing an electronic transaction, comprising:
   (a) receiving a long-term certificate;
   (b) authenticating a user associated with the long-term certificate;
   (c) sending a short-term certificate to the user authenticated in (b).

2. The method of claim 1, further comprising:
   (d) evaluating a risk associated with the user; and
   (e) including in the short-term certificate information about the risk associated with the user.

3. The method of claim 2, wherein the risk associated with the user is reflected in an upper limit on the short-term certificate's value.

4. The method of claim 1, further comprising:
   (d) receiving information about the user's spending history; and
   (e) including in the short-term certificate information based on the user's spending history.

5. The method of claim 4, wherein the information about a user's spending history includes marketing offers.

6. The method of claim 1, further comprising:
   (d) receiving from a market partner information about the market partner's needs; and
   (e) including in the short-term certificate information about

the market partner's needs.

7. The method of claim 6, wherein the information about a market partner's needs includes marketing offers.

8. The method of claim 2, further comprising:

(f) receiving, information about the user's spending habits; and

(g) including in the short-term certificate information about the user's spending habits.

9. The method of claim 2, further comprising:

(f) receiving from a market partner information about the market partner's needs; and

(g) including in the short-term certificate information about the market partner's needs.

10. The method of claim 4, further comprising:

(f) receiving from a market partner information about the market partner's needs; and

(g) including in the short-term certificate information about the market partner's needs.

11. The method of claim 8, further comprising:

(h) receiving from a market partner information about the market partner's needs; and

(i) including in the short-term certificate information about the market partner's needs.

12. The method of claim 1, further comprising:

(d) billing the user through a regular billing channel between the certifier and the user.

13. The method of claim 12, wherein the regular billing channel is a telephone bill.

14. The method of claim 12, wherein the regular billing channel is a credit-card bill.

15. The method of claim 8, further comprising:

(h) billing the user through a regular billing channel between the certifier and the user.

16. The method of claim 11, further comprising:

(j) billing the user through a regular billing channel between the certifier and the user.

17. An apparatus for practicing commerce on a network, comprising:

(a) a processor;

(b) a port coupled to said processor; and

(c) a memory, also coupled to said processor, storing instructions adapted to be executed by said processor to

(i) receive a long-term certificate;

(ii) authenticate a user associated with the long-term certificate; and

(iii) send short-term certificates to the user authenticated in (ii).

18. The apparatus of claim 17, further comprising:

(d) a memory storing instructions adapted to be executed by

said processor to

(i) evaluate the risk associated with the user; and

(ii) include in the short-term certificate information about the risk associated with the user.

19. The apparatus of claim 18, wherein the risk associated with the user is reflected in an upper limit on a value of the short-term certificate.

20. The apparatus of claim 17, further comprising:

(d) a memory storing instructions adapted to be executed by said processor to

(i) receive information about the user's spending history; and

(ii) include in the short-term certificate information based on the user's spending history.

21. The apparatus in claim 20, wherein the information about the user's spending habits includes marketing offers.

22. The apparatus of claim 17, further comprising:

(d) a memory storing instructions adapted to be executed by said processor to

(i) receive from a market partner information about the market partner's needs; and

(ii) include in the short-term certificate information about the market partner's needs.

23. The apparatus of claim 22, wherein the information about the market partner's needs includes marketing offers.

24. The apparatus of claim 18, further comprising:

(e) a memory storing instructions adapted to be executed by said processor to

(i) receive information about the user's spending habits; and

(ii) include in the short-term certificate information about the user's spending habits.

25. The apparatus of claim 18, further comprising:

(e) a memory storing instructions adapted to be executed by said processor to

(i) receive from a market partner information about the market partner's needs; and

(ii) include in the short-term certificate information about the market partner's needs.

26. The apparatus of claim 20, further comprising:

(e) a memory storing instructions adapted to be executed by said processor to

(i) receive from a market partner information about the market partner's needs; and

(ii) include in the short-term certificate information about the market partner's needs.

27. The apparatus of claim 24, further comprising:

(e) a memory storing instructions adapted to be executed by

said processor to

(i) receive from a market partner information about the market partner's needs; and

(ii) include in the short-term certificate information about the market partner's needs.

28. A computer-readable medium that stores instructions adapted to be executed by a processor to perform the steps of:

(a) receiving a long-term certificate;

(b) authenticating a user associated with the long-term certificate;

(c) sending a short-term certificate to the user authenticated in (b).

29. The computer-readable medium of claim 28, further comprising

(d) evaluating the risk associated with the user; and

(e) including in the short-term certificate information about the risk associated with the user.

30. The computer-readable medium of claim 28, further comprising:

(d) receiving information about the user's spending history; and

(e) including in the short-term certificate information about the user's spending history.

31. The computer-readable medium of claim 28, further comprising:

(d) receiving from a market partner information about the market partner's needs'

(e) including in the short-term certificate information about the market partner's needs.

FIG. 1

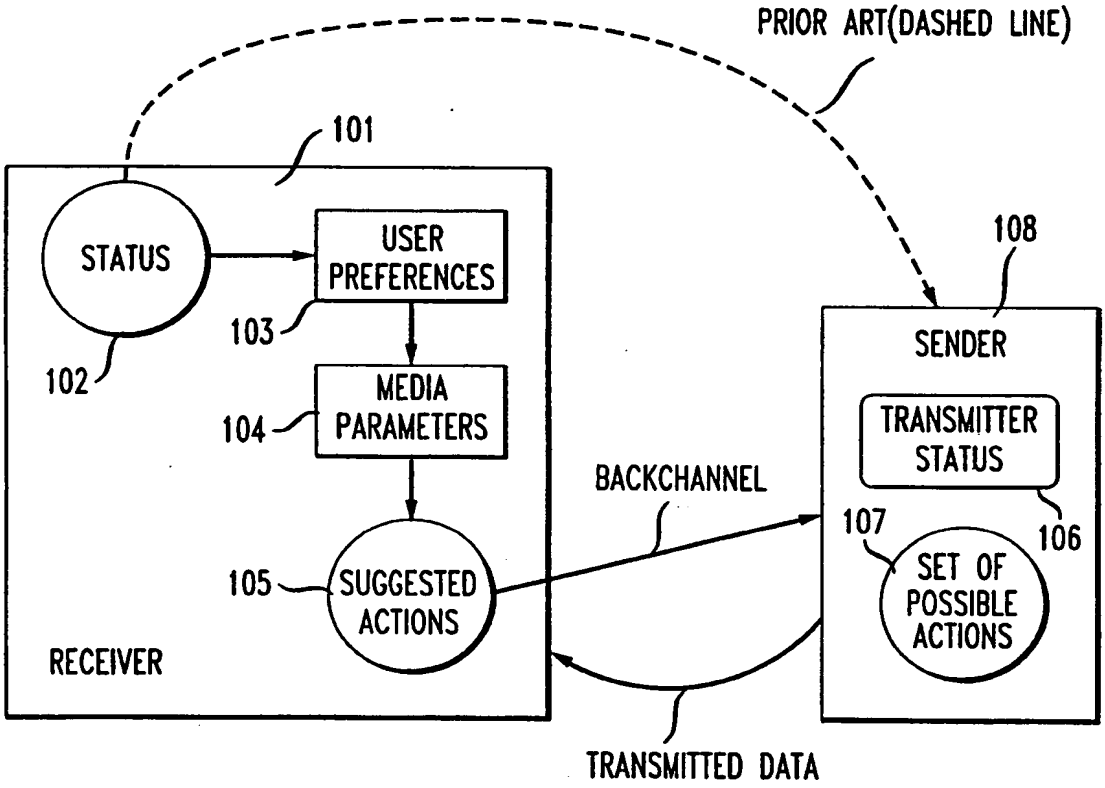

PRIOR ART(DASHED LINE)
101
STATUS
USER PREFERENCES
103
102
MEDIA PARAMETERS
104
105
SUGGESTED ACTIONS
RECEIVER
BACKCHANNEL
108
SENDER
TRANSMITTER STATUS
107
106
SET OF POSSIBLE ACTIONS
TRANSMITTED DATA

FIG. 2

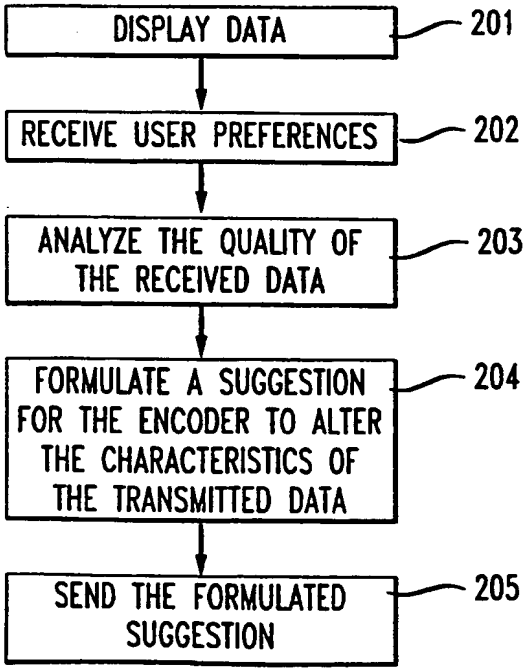

DISPLAY DATA
201
RECEIVE USER PREFERENCES
202
ANALYZE THE QUALITY OF THE RECEIVED DATA
203
FORMULATE A SUGGESTION FOR THE ENCODER TO ALTER THE CHARACTERISTICS OF THE TRANSMITTED DATA
204
SEND THE FORMULATED SUGGESTION
205

FIG. 3

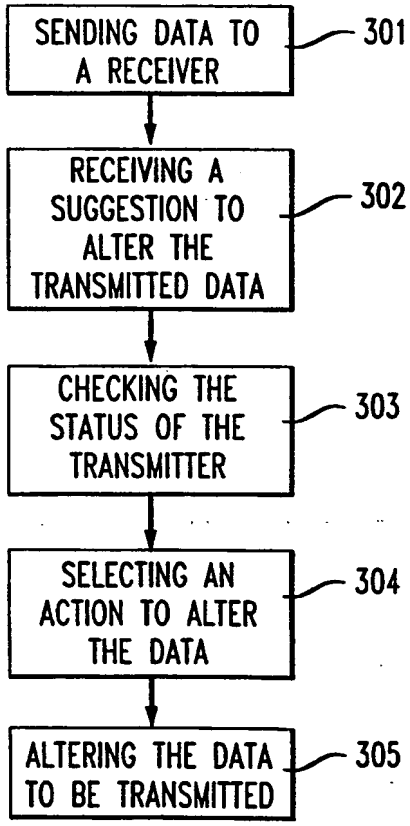

SENDING DATA TO A RECEIVER
301
RECEIVING A SUGGESTION TO ALTER THE TRANSMITTED DATA
302
CHECKING THE STATUS OF THE TRANSMITTER
303
SELECTING AN ACTION TO ALTER THE DATA
304
ALTERING THE DATA TO BE TRANSMITTED
305

FIG. 4

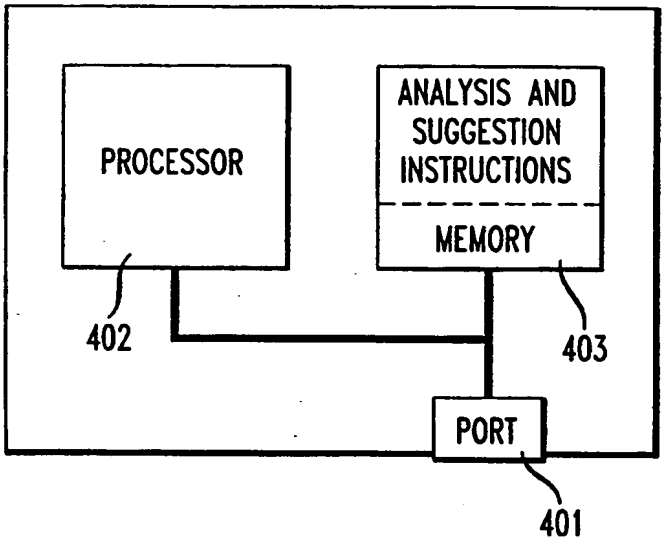
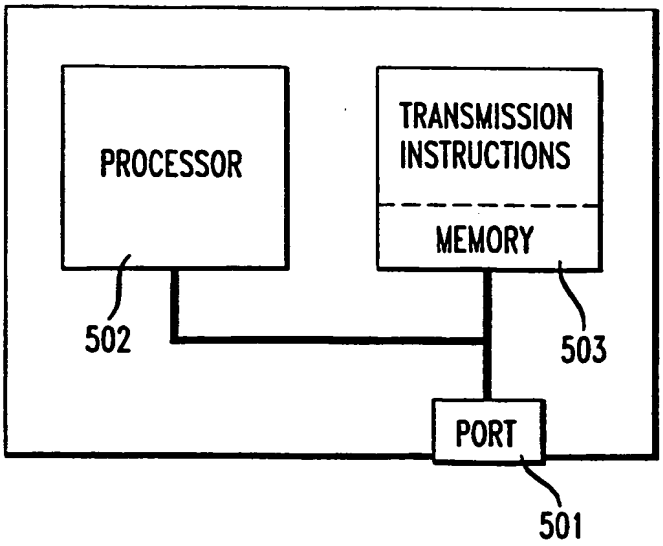

PROCESSOR
ANALYSIS AND SUGGESTION INSTRUCTIONS
MEMORY
402
403
PORT
401

FIG. 5


PROCESSOR
TRANSMISSION INSTRUCTIONS
MEMORY
502
503
PORT
501

INTERNATIONAL SEARCH REPORT

Internat. / Application No
PCT/US 98/19717

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 671 279 A (ELGAMAL TAHER) 23 September 1997 see abstract see column 3, line 26 - line 57 see column 7, line 45 - column 8, line 21 see column 15, line 29 - line 41 see column 17, line 17 - line 30 see column 19, line 40 - line 52 see figure 1	1,12,14
A	WO 97 03410 A (EGENDORF ANDREW) 30 January 1997 see page 3, line 12 - page 7, line 3 see page 15, line 20 - page 18, line 21	12-16
A	WO 96 39668 A (INTERACTIVE MEDIA WORKS L L C ;TOADER ADRIAN (US)) 12 December 1996	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 March 1999	30. 03. 1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bocage, S

4

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat. Application No
PCT/US 98/19717

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 738 058 A (BARKAN MORDHAY) 16 October 1996	

4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 98/19717

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 98/19717

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

There appears to be a lack of correspondence between the drawings as present in the application and the relevant parts of the description. The application a whole is therefore not clear (Article 17(2)(b) together with Articles 5 and 7). Nevertheless, as far as the application can be understood from the claims and description a meaningful search has been carried out.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internat. Application No
PCT/US 98/19717

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5671279 A	23-09-1997	NONE	
WO 9703410 A	30-01-1997	US 5794221 A	11-08-1998
		AU 5986596 A	10-02-1997
		CA 2226253 A	30-01-1997
		EP 0845125 A	03-06-1998
WO 9639668 A	12-12-1996	US 5774869 A	30-06-1998
		US 5806043 A	08-09-1998
		US 5749075 A	05-05-1998
		AU 6029296 A	24-12-1996
		CA 2223787 A	12-12-1998
EP 0738058 A	16-10-1996	US 5864667 A	26-01-1999